UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/710,307 | 07/01/2004 | David S. Bonalle | 70655.1300 | 4306 |

66170 7590 04/10/2007

AMERICAN EXPRESS TRAVEL RELATED SERVICES CO., INC.
c/o SNELL & WILMER, L.L.P.
ONE ARIZONA CENTER
400 E. VAN BUREN STREET
PHOENIX, AZ 85004-2202

| EXAMINER | |
|---|---|
| WALSH, DANIEL I | |
| **ART UNIT** | **PAPER NUMBER** |
| 2876 | |

| SHORTENED STATUTORY PERIOD OF RESPONSE | MAIL DATE | DELIVERY MODE |
|---|---|---|
| 3 MONTHS | 04/10/2007 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

TH

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/710,307 | BONALLE ET AL. | |
| | Examiner | Art Unit | |
| | Daniel I. Walsh | 2876 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *1-10-07 (RCE)*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-5,7-9,12-20 and 22-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5,7-9,12-20 and 22-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on ____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *1-07*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

1. Receipt is acknowledged of the IDS (4) received on 1-18-07.

The information disclosure statement filed 1-18-07 fails to comply with 37 CFR 1.98(a)(3) because it does not include a concise explanation of the relevance, as it is presently understood by the individual designated in 37 CFR 1.56(c) most knowledgeable about the content of the information, of each patent listed that is not in the English language. It has been placed in the application file, but the information referred to therein has not been considered.

### *Claim Rejections - 35 USC § 103*

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

2. Claims 1-5, 7-9, 12-13, 15, 17-19, and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Black (US 2005/0122209) in view of Hoshino (US 6,636,620).

Re claim 1, Black teaches a smartcard transaction system configured with a biometric security device, the system comprising: a smartcard configured to communicate with a reader, wherein the reader and biometric security device communicate with a host; a biometric security device comprising a biometric sensor configured to detect a proffered biometric sample, the biometric sample configured to communicate with the system; and a means to verify (verification device) the proffered biometric sample to facilitate a transaction (FIG. 1C, which teaches a smartcard (abstract), smartcard reader, biometric sensor (step 6 of FIG. 1C), and steps 7+ which teach authentication and to facilitate a transaction (by a device)). Though Black is silent to a specific verification device, the Examiner notes that Black teaches verification/authentication, and therefore it would have been obvious to one of ordinary skill in the art to use a verification device to verify that the sample is an authentic biometric sample, for increased security. The Examiner notes that such devices are conventional in the art and therefore are obvious expedients.

Black is silent to generating data representing the samples, and to use such data as a variable in an encryption calculation to secure user/transaction data.

Hoshino teaches encryption of biometric data (claim 3).

At the time the invention was made, it would have been obvious to one of ordinary skill in the art to combine the teachings of Black with those of Hoshino.

One would have been motivated to do this for more security.

The Examiner has interpreted that the proffered sample is used as a variable in an encryption calculation as it is offered up/data is generated representing the sample, and that such data is used as a variable together with the encrypted information, to verify a users identity.

Re claim 2, Black teaches the sensor is configured to communicate with the system via at least one of a smartcard, a reader, and a network (FIG. 1C).

Re claims 3, and 16, as the data is used in an encryption scheme, the Examiner notes that the selection of a particular type of scheme, would have been an obvious to one of ordinary skill in the art based on the type/level of security.

Re claim 4, Black teaches that the digital and electronic signatures are captured and preserved in a transaction record (paragraph [0125]). This is interpreted to include logging at least one of a detected biometric sample, processed biometric sample, and stored biometric sample. Though Black is silent to the biometric sensor doing the logging, the Examiner notes that it would have been obvious for the sensor to do the logging, since it captures/receives the inputs. Additionally, though silent to security procedures when the data doesn't match, the Examiner notes that it is well known and conventional to allow users a couple attempts to access a system before performing a security procedure (3 attempts at a password, PIN, etc. before blocking access for a predetermined time). It would have been obvious to allow the user a couple attempts before blocking the user, transponder, etc. to provide the user an attempt to rectify a mistake made during providing biometric information. Such means are well known and conventional in the art for access control, and employing them in a biometric system is an obvious expedient to provide security, while also allowing a user more than one attempt at access in case a mistake is made.

Re claim 5, Black teaches that a data packet is stored remotely (host computer) where the data packet includes at least one of proffered and registered biometric samples proffered and registered user information, terrorist information, and criminal information (paragraph [0125], FIG. 10A-11B and 14A-14B). The Examiner notes that though such data packet/information is shown with reference to a transponder/RFID, Black states that the device can be a smartcard, transponder, etc. (abstract). Accordingly, it is obvious that such teachings can be applied to smartcards to produce expected results for data storage and retrieval for verifying a transaction using biometrics, especially since it has been taught that such information can be stored on the transponder/card itself or remotely (for security reasons) (paragraph [0090]+). Though silent to a database, the Examiner notes that storing records on a computer in a database is an obvious expedient, well within the skill in the art to organize data for efficient comparison and retrieval.

Re claim 7, though silent to a message authentication code, it is understood that if authentication is performed that a message/form of notification is created, thus broadly interpreted as a message authentication code being generated (a communication that authentication failed/succeeded). One would have been motivated to generate such a code in order to signify authentication/verification.

Re claim 8, Black teaches a device configured to compare a proffered biometric sample with a stored biometric sample (FIG. 1C ).

Re claim 9, Black teaches a device configured to compare at least one characteristic of a biometric sample including at least one of minutia, vascular patterns, prints, waveforms, odorants, nodal points, reference points, size, shape, thermal patterns, blood flow, and body heat (FIG. 1C which teaches comparison of fingerprint and signature).

Re claim 12, Black teaches a registered biometric sample is associated with at least one of personal information, credit card information, debit card information, savings account information, membership information, PayPal account information, Western Union account information, electronic bill payment information, automatic bill payment information and loyalty point information (abstract, as an account is linked with the biometrics provided during a registration).

Re claim 13, as Black teaches different people using the system with different biometrics, it is obvious that each different sample would be associated with a different account, because different peoples samples would be unique, and each person could have a sample linked to an account.

Re claim 15, as Black teaches that an account is only accessed after a sample is verified, it is interpreted as beginning authentication after the sample is verified.

Re claim 17, though Black is silent to the sensor providing notification upon detection of a sample, the Examiner notes that it is well within the skill in the art to provide notification that a sample has been detected/received (see previous Office Actions reference to Janiak et al.). Though Black is silent to providing notification that a primary account is being accessed, the Examiner notes that the failure to detect a sample/fail to verify a sample, would be evident to the user by a lack of response or a rejected attempt. Positive notification is merely an equivalent. Further, the Applicant has not shown that positive notification of sample detecting would materially affect the workings of the invention, as compared with what can be considered passive notification. The Examiner notes that merely providing notification that the account is being accessed (to the customer/store employee for example) is well known and conventional in the art

as evidenced through conventional debit/credit card transactions which indicate to users/workers that authorization is occurring, and through processing and completion of the transaction, positive notification is provided (such as through text, audio, visual, or mere completion of the transaction). It would have been obvious to one of ordinary skill in the art to provide such information, in order to keep the customer/worker aware of the status of the transaction.

Re claim 18, Black teaches the device configured to verify/authenticate an individual for purchasing of goods (abstract) and hence is interpreted as substantially simultaneous access to goods.

Re claim 19, as it has been discussed above re Baer that transactions above a certain amount require a certain biometric, the Examiner has interpreted such teachings as overriding a rule as claimed. As such, as the transactions are conventionally logged, it would have been obvious to report all transactions, including those over a certain amount (requiring a biometric) to the host for record keeping.

Re claim 20, the Examiner notes that preset transaction limitations are known to be associated with a card, and therefore associated by extension to the biometric, such as a maximum credit line/credit purchase, as is conventional in the art for security.

3. Claims 1, 3 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Black/Hoshino, as discussed above, in view of Brandys (US 2002/0186838).

The teachings of Black have been discussed above.

Black/Hoshino is silent to using the data representing the sample as one of a private/public key.

Brandys teaches such limitations (abstract).

At the time the invention was made, it would have been obvious to one of ordinary skill in the art to combine the teachings of Black/Hoshino with those of Brandys.

Though silent to a particular encryption algorithm, the use of encryption algorithms for enhanced security are understood, and therefore selection of a particular type would be an obvious expedient, based on system constraints, desired security, etc.

4. Claims 1, 3, 7, 16, and 23 are is rejected under 35 U.S.C. 103(a) as being unpatentable over Black, as discussed above, in view of Hohle et al. (US 6,101,477).

The teachings of Black have been discussed above.

Black is silent to the specifics of the encryption and MAC creating.

Hohle et al. teaches such encryption (col 21, lines 63+) and MAC (col 22, lines 47+).

At the time the invention was made, it would have been obvious to one of ordinary skill in the art to combine the teachings of Black with Hohle et al.

One would have been motivated to do this for enhanced security.

Though silent to asymmetric/symmetric algorithms, the Examiner notes that the selection of a particular type of encryption algorithm/scheme is well within the skill in the art based on desired security, system constraints, etc.

5. Claim 14 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Black/Hohle et al., as discussed above, in view of de Sylva.

Re claim 14 the teachings of Black/Hohle et al. have been discussed above.

Black/Hohle et al. is silent to the sample being primarily associated with a first user account and secondarily associated with another account, different from the first.

De Sylva teaches such limitations through the use account record 30.

At the time the invention was made, it would have been obvious to one of ordinary skill in the art to combine the teachings of Black/Hohle et al. with those of de Sylva.

One would have been motivated to do this to have additional accounts associate with a sample for more flexibility and customization for the user.

Re claim 19, Black teaches the device configured to verify is configured to facilitate the use of at least one secondary security procedure (signature, metrics FIG. 1C). Black teaches the use of a transaction record (paragraph [0125]) but it silent to the record occurring during unauthorized access attempts. However, the Examiner notes it would have been obvious to one or ordinary skill in the art to store such attempts in order to obtain security information regarding usage and attempts to access accounts illegally. Additionally, the Examiner notes that it is understood that if access is blocked due to improper authentication, the host would be area of this because the host is the entity through which authentication occurs, and storing such information would have been obvious for security reasons (detecting fraud attempts, system breaches, etc).

Black is silent to the verification device sending a signal to the host device to notify that an established rules for the transponder is being violated.

De Sylva teaches remote database 32 stores non-authenticated data from the verifier (50) (paragraph [0032]).

At the time the invention was made, it would have been obvious to one of ordinary skill in the art to combine the teachings of Black/Baer with those of de Sylva.

One would have been motivated to do this in order to alert instances of fraud. It would have been obvious for the verification device to complete such steps, as it is responsible for

verifying the sample, if the sample is not verified it would be obvious to create notification for fraud.

6. Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over Black/Hohle et al., as discussed above, in view of Moebs et al. (US 2005/0065872).

Re claim 14 the teachings of Black/Hohle et al. have been discussed above.

Black/Hohle et al. is silent to the sample being primarily associated with a first user account and secondarily associated with another account, different from the first.

Moebs et al. teaches such limitations (paragraph [0017]).

At the time the invention was made, it would have been obvious to one of ordinary skill in the art to combine the teachings of Black/Baer with those of Moebs et al.

One would have been motivated to do this to have overdraft protection.

7. Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over Black/Hohle et al., as discussed above, in view of Jensen et al. (US 2005/0165684).

The teachings of Black/Hohle et al. have been discussed above.

Black/Hohle et al. are silent to notifying the hose if a rule is violated (to be violated).

Jensen et al. teaches that a sample is required to violate a transaction rule (paragraph [0081]).

At the time the invention was made, it would have been obvious to one of ordinary skill in the art to combine the teachings of Black/Hohle et al. with those of Jensen et al., for additional security. The Examiner notes it would have been obvious to notify the host, as the host provides authentication/authorization for transactions. .

9. Claims 1 and 22-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Black (US 2005/0122209) in view of Hohle et al. (US 6,101,477).

Black teaches a smartcard transaction system configured with a biometric security device, the system comprising: a smartcard configured to communicate with a reader, wherein the reader and biometric security device communicate with a host; a biometric security device comprising a biometric sensor configured to detect a proffered biometric sample, the biometric sample configured to communicate with the system; and, a means to verify the proffered biometric sample to facilitate a transaction (FIG. 1C, which teaches a smartcard (abstract), smartcard reader, biometric sensor (step 6 of FIG. 1C), and steps 7+ which teach authentication and to facilitate a transaction (by a device)). Though Black is silent to a specific verification device, the Examiner notes that it would have been obvious to one of ordinary skill in the art to use a verification device to verify that the sample is an authentic biometric sample, for increased security. The Examiner notes that such devices are conventional in the art and therefore are obvious expedients.

Black is silent to the details of the applications and file structures as claimed.

Hohle et al. teaches such limitations (see claim 1).

At the time the invention was made, it would have been obvious to one of ordinary skill in the art to combine the teachings of Black with those of Hohle et al.

One would have been motivated to do this for convenience (applications for user).

It would have been obvious to verify the transaction using the file structure as claimed, as taught by Hohle et al., because the structure stores the relevant information. Hohle et al. teaches message authentication codes (col 22, lines 47+). The use of a key has been discussed above re

Hohle et al. as well, as a means for encryption/security. The use of such means are an obvious expedient for enhanced security, thus it would have been obvious to one of ordinary skill in the art to combine the teachings of Black with those of Hohle et al. for security purposes.

10. Claim 24 is rejected under 35 U.S.C. 103(a) as being unpatentable over Black, a s discussed above, in view of Hoshino as discussed above.

The teachings of Black have been discussed above.

Black is silent to encryption.

Hoshino teaches such limitations as discussed above.

It would have been obvious to one of ordinary skill in the art to combine the teachings of Black with those of Hoshino.

One would have been motivated to do this for enhanced security.

### *Additional Remarks*

11. The Examiner notes that encryption of data is well known and conventional in the art for security. The Examiner also notes that Hohle et al. teaches MAC (message authentication code, as per claims 7 and 23) and encryption, Hoshino also teaches encryption, and the Examiner contends that at a specific type of encryption algorithm is an obvious expedient to one of ordinary skill in the art based on a security level or system constraint (re claim 16).

### *Conclusion*

12. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure (see PTO-892).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure (see attached PTO-892).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Daniel I. Walsh whose telephone number is (571) 272-2409. The examiner can normally be reached on M-F 7:30-4:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Michael G. Lee can be reached on (571) 272-2398. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Daniel I Walsh
Examiner
Art Unit 2876
3-30-07

DANIEL WALSH
PRIMARY EXAMINER